FortiOS - VMware ESXi Cookbook

Version 6.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

March 28, 2019
FortiOS 6.2 VMware ESXi Cookbook
01-620-543863-20190328

TABLE OF CONTENTS

About FortiGate-VM on VMware ESXi

This guide describes how to deploy a FortiGate virtual appliance in a VMware ESXi environment. This includes how to configure the virtual hardware settings of the virtual appliance.

FortiGate virtual appliances allow you to mitigate blind spots by implementing critical security controls within your virtual infrastructure. They also allow you to rapidly provision security infrastructure whenever and wherever it is needed. FortiGate virtual appliances feature all of the security and networking services common to traditional hardware-based FortiGate appliances. With the addition of virtual appliances from Fortinet, you can deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform.

FortiGate virtual appliance models and licensing

Fortinet offers the FortiGate-VM in five virtual appliance models, which are determined by license. When configuring the FortiGate-VM, ensure that the hardware settings are within the ranges outlined below. Contact your Fortinet-authorized reseller for more information.

The following summarizes FortiGate-VM model information:

Technical specification	FG-VM00	FG-VM01	FG-VM02	FG-VM04	FG-VM08
Virtual CPUs (minimum/maximum)	1/1	1/1	1/2	1/4	1/8
Virtual network interfaces (minimum/maximum)	2/10				
Virtual memory (minimum/maximum)	1 GB/2 GB	1 GB/2 GB	1 GB/4 GB	1 GB/6 GB	1 GB/12 GB
Virtual storage (minimum/maximum)	32 GB/2 TB				
Managed wireless access points (tunnel mode/global)	32/32	32/64	256/512	256/512	1024/4096
Virtual domains (default/maximum)	1/2	10/10	10/25	10/50	10/250

The minimum and maximum values can change. In this case, manually change the VM settings to accommodate the new parameters.

When you submit an order for a FortiGate-VM virtual appliance, a license registration code is sent to the email address entered on the order form. Use this code to register the FortiGate-VM virtual appliance with Customer Service & Support, and then download the license file. After you upload the license to the FortiGate-VM virtual appliance and validate it, your FortiGate-VM virtual appliance is fully functional.

The number of virtual network interfaces does not solely depend on the FortiGate-VM. Some virtual environments have their own limitations on the number of interfaces allowed.

FortiGate-VM virtual appliance evaluation license

he FortiGate-VM virtual appliance includes a limited, 15-day evaluation license that supports:

- 1 CPU maximum
- 1024 MB memory maximum
- Low encryption only (no HTTPS administrative access)
- All features except FortiGuard updates

Note the following:

- Attempting to upgrade the FortiGate firmware will lock the web-based manager until you upload a full license.
- Technical support is not included. The trial period begins the first time you start the FortiGate-VM.
- After the trial license expires, functionality is disabled until you upload a full license file.

FortiOS FortiGate-VM virtual appliance licenses

The primary requirement for provisioning a virtual FortiGate may be the number of interfaces that it can accommodate rather than its processing capabilities. In some cloud environments, the options with a high number of interfaces tend to have high numbers of virtual CPUs (vCPUs).

The licensing for FortiGate-VM does not restrict whether the FortiGate can work on a VM instance in a public cloud that uses more vCPUs than the license allows. The number of vCPUs indicated by the license does not restrict the FortiGate from working, regardless of how many vCPUs are included in the virtual instance. However, only the licensed number of vCPUs process traffic and management tasks. The rest of the vCPUs are unused.

License	1 vCPU	2 vCPU	4 vCPU	8 vCPU	16 vCPU	32 vCPU
FGT-VM08	OK	OK	OK	OK	8 vCPUs used for traffic and management. The rest are unused.	8 vCPUs used for traffic and management. The rest are unused.

You can provision a VM instance based on the number of interfaces you need and license the FortiGate-VM for only the processors you need.

The behavior differs between private and public clouds:

- Private clouds: both licensed vCPUs and RAM are affected
- Public clouds: only licensed vCPU is affected

For example, you can activate FG-VM02 on a FGT-VM with 4 vCPUs with 16 GB of RAM, running on a private VM platform. Only 2 vCPU and 4 GB of RAM, as licensed, will be consumable.

Likewise, you can activate FG-VM02 on a FGT-VM c5.2xlarge EC2 instance with 8 vCPUs running on AWS. Only 2 vCPU will be consumable, and there is no limit on the RAM size. Licenses for public clouds are also referred to as Bring Your Own License (BYOL).

Preparing for deployment

This guide assumes that before deploying the FortiGate-VM virtual appliance on the VMware ESXi virtual platform, you have addressed the following requirements:

Virtual environment

The ESXi software is installed on a physical server with sufficient resources to support the FortiGate-VM and all other VMs that will be deployed on the platform.

If the FortiGate-VM will be configured to operate in transparent mode or will be included in a FortiGate Clustering Protocol (FGCP) High Availability (HA) cluster, ensure that the VMware virtual switches have been configured to support the operation of the FortiGate-VM before you create the FortiGate-VM. See Transparent mode on page 16 or High Availability on page 16.

Management software

The VMware management software, vSphere, is installed on a computer with network access to the ESXi server.

Connectivity

An Internet connection is required for the FortiGate-VM to contact FortiGuard to validate its license. If the FortiGate-VM is in a closed environment, it must be able to connect to a FortiManager to validate the FortiGate-VM license. See "Validating the FortiGate-VM license with FortiManager".

Configuring resources

Before you start the FortiGate-VM for the first time, ensure that you have configured the following resources as the FortiGate-VM virtual appliance license specifies:

- Disk sizes
- CPUs
- RAM
- Network settings

To configure the resources for a FortiGate-VM deployed on VMware ESXi, use the vSphere client.

Registering the FortiGate-VM virtual appliance

Registering the FortiGate-VM virtual appliance with Customer Service & Support allows you to obtain the FortiGate-VM virtual appliance license file.

1. Log into Customer Service & Support using a support account, or select *Sign Up* to create an account.
2. Go to *Asset* > *Register/Renew*.
3. Enter the registration code that was emailed to you, and select *Register* to access the registration form.
4. Complete and submit the registration form.
5. In the registration acknowledgment page, click the *License File Download* link.
6. Save the license file (.lic) to your local computer. See Uploading the FortiGate-VM virtual appliance license on page 13 or Validating the FortiGate-VM virtual appliance license with FortiManager on page 14 for information about uploading the license file to your FortiGate-VM via the web-based manager.

Downloading the FortiGate-VM virtual appliance deployment package

FortiGate-VM deployment packages are found on the Customer Service & Support site.

1. Go to the Customer Service & Support site.
2. From the *Download* dropdown list, select *VM Images* to access available VM deployment packages.
3. From the *Select Product* dropdown list, select *FortiGate*.
4. From the *Select Platform* dropdown list, select *VMware ESXi*.
5. Select the desired FortiOS version. There are two files available for download: the file required to upgrade from an earlier version and the file required for a new deployment.
6. Click Download and save the file.

For more information, see the FortiGate product datasheet.

You can also download the following resources for the firmware version:

- *FortiOS Release Notes*
- FORTINET-FORTIGATE MIB file
- FSSO images
- SSL VPN client

Deployment package contents for VMware ESXi

You must create a 32 GB lod disk.

The FortiGate-VM virtual appliance deployment package contains the following components:

- fortios.vmdk: FortiGate-VM system hard disk in VMDK format
- datadrive.vmdk: FortiGate-VM log disk in VMDK format

- Open Virtualization Format (OVF) template files:
  - FortiGate-VM64.ovf: OVF template based on Intel e1000 NIC driver
  - FortiGate-VM64.hw04.ovf: OVF template file for older (v3.5) VMware ESX server
  - FortiGate-VMxx.hw07_vmxnet2.ovf: OVF template file for VMware vmxnet2 driver
  - FortiGate-VMxx.hw07_vmxnet3.ovf: OVF template file for VMware vmxnet3 driver

Use the VMXNET3 interface (FortiGate-VMxx.hw07_vmxnet3.ovf template) if the virtual appliance will distribute workload to multiple processor cores.

Deploying and setting up the FortiGate-VM

Before you deploy a virtual appliance, ensure that the requirements described in Preparing for deployment on page 8 are met and that the correct deployment package is extracted to a folder on the local computer (see Downloading the FortiGate-VM virtual appliance deployment package on page 9).

After you deploy a FortiGate-VM and upload a full license to replace the default evaluation license, you can power on the FortiGate-VM and test connectivity.

Deploying the FortiGate-VM

Use the vSphere client to deploy the FortiGate OVF template and create the FortiGate-VM on the VMware ESXi server.

1. Launch the vSphere client, enter your VMware server's IP address or hostname and your username and password, and then select *Login*.
2. In the vSphere client homepage, select *File* > *Deploy OVF Template* to start the OVF Template wizard.
3. Configure the FortiGate-VM deployment:
   a. In the *Source* page, select the source location of the OVF file, select *Browse* to locate the OVF file on your computer, and then select *Next*.
   b. In the *Details* page, verify the OVF template details (product name, download size, size on disk, and description), and then select *Next*.
   c. Read the end user license agreement for FortiGate-VM, select *Accept*, then select *Next*.
   d. In the *Name and Location* page, enter a name for this OVF template, and then select *Next*. The name must be unique within the inventory folder and can contain up to 80 characters.
   e. In the *Disk Format* page, select one of the disk format options, then select *Next*. See the table below for disk format options:

Option	Description
Thick provision lazy zeroed	Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
Thick provision eager zeroed	Allocates the disk space statically (no other volumes can take the space), and writes zeros to all blocks.
Thin provision	Allocates the disk space only when a write occurs to a block, but the total volume size is reported by VMFS to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Once a thin provisioned block is allocated, it remains on the volume regardless of whether you have deleted data, etc.

   f. In the *Network Mapping* page, map the networks used in this OVF template to networks in your inventory, and then select *Next*. Network 1 maps to the FortiGate-VM's port1. You must set the destination network for this entry to access the device console.

g. In the *Ready to Complete* page, review the template configuration, and ensure that Power on after deployment is disabled.

4. Click *Finish*. The message *Deployment Completed Successfully* appears.
5. Upload the license file.
6. Connect the FortiGate-VM to the network.

Initial settings

After you deploy a FortiGate-VM on the VMware ESXi server, perform the following tasks:

- Connect the FortiGate-VM to the network so that it can process network traffic and maintain the license validity.
- Connect to the FortiGate-VM GUI via a web browser for easier administration.
- Ensure that the full license file is uploaded to the FortiGate-VM.
- If you are in a closed environment, enable validation of the FortiGate-VM virtual appliance license against a FortiManager on your network.

The first time you start the FortiGate-VM, you will have access only through your VMware server environment's console window. After you configure one FortiGate network interface with an IP address and administrative access, you can access the FortiGate-VM web-based manager.

Configuring port1

VM platform or hypervisor management environments include a guest console window. On the FortiGate-VM, this provides access to the FortiGate console, equivalent to the console port on a hardware FortiGate unit. Before you can access the GUI, you must configure FortiGate-VM port1 with an IP address and administrative access.

1. In your hypervisor manager, start the FortiGate-VM and access the console window. You might need to press `Enter` to see a login prompt.
2. At the FortiGate-VM login prompt, enter the username `admin`. By default there is no password. Press `Enter`.
3. Using CLI commands, configure the port1 IP address and netmask. Also, HTTP access must be enabled because until it is licensed the FortiGate VM supports only low-strength encryption. HTTPS access will not work. See below:

```
config system interface
   edit port1
      set ip 192.168.0.100 255.255.255.0
      append allowaccess http
end
```

You can also use the `append allowaccess` CLI command to enable other access protocols, such as `auto-ipsec`, `http`, `probe-response`, `radius-acct`, `snmp`, and `telnet`. The `ping`, `https`, `ssh`, and `fgfm` protocols are enabled on the port1 interface by default.

4. To configure the default gateway, enter the following CLI commands:

```
config router static
   edit 1
      set device port1
      set gateway <class_ip>
```

```
end
```

You must configure the default gateway with an IPv4 address. The FortiGate-VM must access the Internet to contact the FortiGuard Distribution Network (FDN) to validate its license.

5. To configure your DNS servers, enter the following CLI commands:

```
config system dns
   set primary <primary DNS server>
   set secondary <secondary DNS server>
end
```

The default DNS servers are 208.91.112.53 and 208.91.112.52.

Uploading the FortiGate-VM virtual appliance license

Every Fortinet VM includes a 15-day trial license. During this time the FortiGate-VM operates in evaluation mode. Before using the FortiGate-VM you must enter the license file that you downloaded from Customer Service & Support upon registration.

To upload the FortiGate-VM license file using the GUI:

1. Go to *Dashboard* > *Main*. In the *Virtual Machine* widget, click the *FGVMEV (FortiGate-VM Evaluation) License* icon. This reveals a menu to take you to the *FortiGate VM License* window or to the *FortiGuard Details* window.
2. In the *Evaluation License* dialog box, select *Enter License*.
3. Select *Upload* and locate the license file (.lic) on your computer. Select *OK* to upload the license file.
4. Refresh the browser to log in.
5. Enter admin in the *Name* field and select *Login*. The VM registration status appears as valid in the *License Information* widget after the license is validated by the FDN or FortiManager for closed networks.

Modern browsers can have an issue with allowing connecting to a FortiGate if the encryption on the device is too low. If this happens, use a FTP/TFTP server to apply the license.

To upload the FortiGate-VM license file using the CLI:

You can also upload the license file using the following CLI command:

```
execute restore vmlicense {ftp | tftp} <filenmame string> <ftp server>[:ftp port]
```

The following shows example output when using a TFTP server to install a license:

```
exec restore vmlicense tftp license.lic 10.0.1.2
This operation will overwrite the current VM license!Do you want to continue? (y/n)y
Please wait...Connect to tftp server 10.0.1.2 ...
Get VM license from tftp server OK.
VM license install succeeded.
```

```
Rebooting firewall.
```

Validating the FortiGate-VM virtual appliance license with FortiManager

You can validate your FortiGate VM license with some FortiManager models. To determine whether your FortiManager unit has the VM activation feature, see the FortiManager datasheet's *Features* section.

1. To configure your FortiManager as a closed network, enter the following CLI command on your FortiManager:
```
config fmupdate publicnetwork
   set status disable
end
```
2. To configure the FortiGate-VM to use FortiManager as its override server, enter the following CLI commands on your FortiGate VM:
```
config system central-management
   set mode normal
   set type fortimanager
   set fmg <FortiManager device's IPv4 address>
   set fmg-source-ip <source IPv4 address when connecting to the FortiManager device>
   set include-default-servers disable
   set vdom <enter the name of the VDOM to use when communicating with the FortiManager
        device>
end
```
3. Load the FortiGate-VM license file in the web-based manager. Go to *System Settings* > *Dashboard*. In the *License Information* widget, in the *Registration Status* field, select *Update*. Browse for the .lic license file and select *OK*.
4. To activate the FortiGate-VM license, enter the `execute update-now` CLI command on your FortiGate-VM.
5. To check the FortiGate-VM license status, enter the `get system status` CLI command on your FortiGate-VM. The following output displays:
```
Version: Fortigate-VM v5.0,build0099,120910 (Interim)
Virus-DB: 15.00361(2011-08-24 17:17)
Extended DB: 15.00000(2011-08-24 17:09)
Extreme DB: 14.00000(2011-08-24 17:10)
IPS-DB: 3.00224(2011-10-28 16:39)
FortiClient application signature package: 1.456(2012-01-17 18:27)
Serial-Number: FGVM02Q105060000
License Status: Valid
BIOS version: 04000002
Log hard disk: Available
Hostname: Fortigate-VM
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Distribution: International
Branch point: 511
Release Version Information: MR3 Patch 4
System time: Wed Jan 18 11:24:34 2012
```
Enter the `diagnose hardware sysinfo vm full` command. The following output displays:
```
UUID: 564db33a29519f6b1025bf8539a41e92
valid: 1
```

```
status: 1
code: 200 (If the license is a duplicate, code 401 displays)
warn: 0
copy: 0
received: 45438
warning: 0
recv: 201201201918
dup:
```

In closed environments without Internet access, you must license the virtual FortiGate offline using a FortiManager as a license server. If the FortiGate-VM cannot perform license validation within the license timeout period, which is 30 days, the FortiGate discards all packets, effectively ceasing operation as a firewall.

The license status goes through some status changes before timing out:

Status	Description
Valid	The FortiGate-VM can connect and validate against a FortiManager or FDS.
Warning	The FortiGate cannot connect and validate against a FortiManager or FDS. A check is made against how many days the Warning status has been continuous. If the number is less the 30 days, the status does not change.
Invalid	The FortiGate cannot connect and validate against a FortiManager or FDS. A check is made against how many days the Warning status has been continuous. If the number is 30 days or more, the status changes to Invalid. The firewall ceases to function properly.

There is only a single log entry after the virtual FortiGate cannot access the license server for the license expiration period. This means that when you go searching the logs for a reason for the FortiGate being offline there will not be a long list of error logs that draw attention to the issue. There is only one entry.

Testing connectivity

Use any of the following methods to power on the FortiGate-VM:

- Select the FortiGate-VM in the inventory list, and select *Power on the virtual machine* on the *Getting Started* tab.
- In the inventory list, right-click the FortiGate-VM and select *Power* > *Power On*.
- Select the FortiGate-VM and click the *Power On* button on the toolbar.

To test connectivity to other devices, using the ping utility is the usual method. For this, you need the FortiGate-VM console. Select the *Console* tab to access the FortiGate-VM console. To enter text, click in the console window. This captures the mouse pointer; however, as the FortiGate-VM console is text-only, the pointer is not visible. To release the pointer, press `Ctrl-Alt`.

In FortiOS, the command for the ping utility is execute ping followed by the IP address you wish to connect to.

Before you configure the FortiGate-VM for use in production, ensure that connections between it and all required resources can be established.

- If the FortiGate-VM will provide firewall protection between your network and the Internet, verify that it can connect to your Internet access point and to resources on the Internet.
- If the FortiGate-VM is part of a Fortinet Security Fabric, verify that it can connect to all devices in the Security Fabric.
- Verify that each node on your network can connect to the FortiGate-VM.

For information about configuring and operating the FortiGate-VM after it has been successfully deployed and started on the hypervisor, see the *FortiOS documentation*.

Transparent mode

If the FortiGate-VM is configured to operate in transparent mode, you must configure the VMware ESXi server's virtual switches to operate in promiscuous mode to allow traffic that is not addressed to the FortiGate-VM to pass through it.

1. In the vSphere client, select your VMware server, and then select the *Configuration* tab.
2. In *Hardware*, select *Networking*.
3. Select vSwitch0's *Properties*.
4. In the *Properties* window, select *vSwitch*, then select *Edit*.
5. On the *Security* tab, set *Promiscuous Mode* to *Accept*, then click *OK*.
6. Click *Close*.
7. Repeat steps 3-6 for other virtual switches that the FortiGate-VM uses.

High Availability

FortiGate-VM HA supports having two VMs in a HA cluster on the same physical platform or different platforms. The primary consideration is that all interfaces involved be able to communicate efficiently over TCP/IP connection sessions.

There are two options for setting up the HA heartbeat: unicast and broadcast. Broadcast is the default HA heartbeat configuration. However, the broadcast configuration may not be ideal for FortGate-VM because it may require special settings on the host. In most cases, unicast configuration is preferred.

The differences between setup for unicast and broadcast heartbeats are:

- Unicast does not change the FortiGate-VM interface MAC addresses to virtual MAC addresses.
- Unicast HA only supports two FortiGate-VMs.
- Unicast HA heartbeat interfaces must be connected to the same network and you must add IP addresses to these interfaces.

Unicast

You can configure unicast settings in the FortiOS CLI. The syntax is as follows:

```
config system ha
   set unicast-hb {enable/disable}
```

```
    set unicast-hb-peerip {IP address of the peer's heartbeat interface}
end
```

Setting	Description
`unicast-hb`	Enable or disable the default unicast HA heartbeat.
`unicast-hb-peerip`	IP address of the HA heartbeat interface of the other FortiGate VM in the HA cluster.

Broadcast

Broadcast HA heartbeat packets are non-TCP packets that use Ethertype values 0x8890, 0x8891, and 0x8890. These packets use automatically assigned link-local IPv4 addresses in the 169.254.0.x range for HA heartbeat interface IP addresses.

For FortiGate-VMs to support a broadcast HA heartbeat configuration, you must configure the virtual switches that connect heartbeat interfaces to operate in promiscuous mode and support MAC address spoofing.

In addition, you must configure the VM platform to allow MAC address spoofing for the FortiGate-VM data interfaces. This is required because in broadcast mode, the FGCP applies virtual MAC addresses to FortiGate data interfaces, and these virtual MAC addresses mean that matching interfaces of the FortiGate-VM instances in the cluster will have the same virtual MAC addresses.

To configure a virtual switch that connects heartbeat interfaces:

1. In the vSphere client, select your VMware server, and then select the *Configuration* tab.
2. In *Hardware*, select *Networking*.
3. Select the virtual switch's *Properties*.
4. In the *Properties* window, select *vSwitch*, then select *Edit*.
5. On the *Security* tab, set *Promiscuous Mode* to *Accept*, then click *OK*.
6. Click *Close*.

You must also configure the virtual switches connected to other FortiGate-VM interfaces to allow MAC address changes and accept forged transmits. This is required because the FGCP sets virtual MAC addresses for all FortiGate-VM interfaces and the same interfaces on the different FortiGate-VM instances in the cluster will have the same virtual MAC addresses.

To configure a virtual switch that connects FortiGate-VM interfaces:

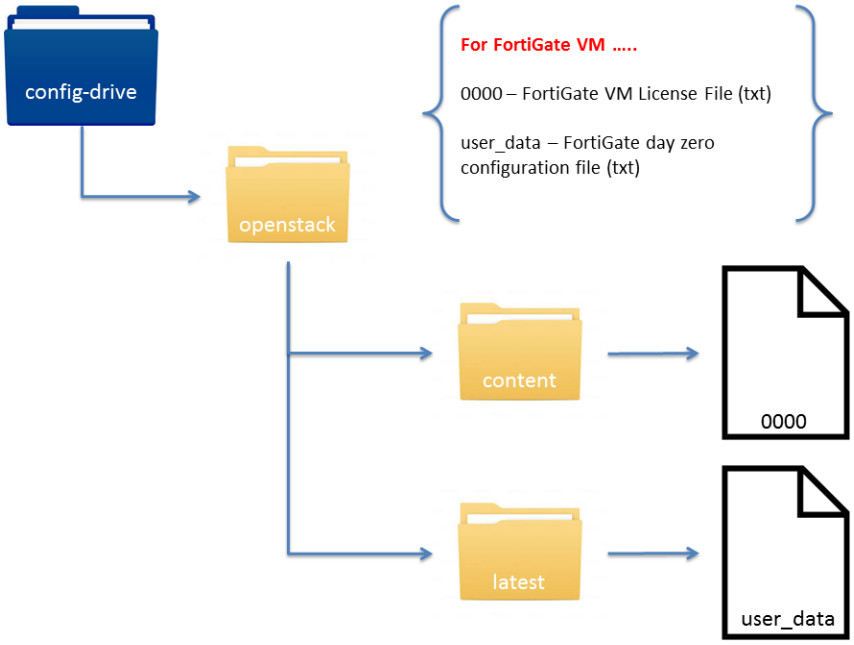
1. In the vSphere client, select your VMware server, and then select the *Configuration* tab.
2. In *Hardware*, select *Networking*.
3. Select the virtual switch's *Properties*.
4. Set *MAC Address Changes* to *Accept*.
5. Set *Forged Transmits* to *Accept*.

Cloud-init using config drive

This section describes how to bootstrap a FortiGate-VM in VMware vCenter using config drive. This recipe is for deploying pre-configured FortiGate-VMs on VMware vCenter or standalone ESX so that they boot with a pre-determined configuration and a valid license.

Ensure that you verify the config drive functionality available for your FortiGate-VM version in the release notes. FortiGate-VM 5.4.1 and above support version 2 of the config-drive capabilities. Cloud-Init config drive was initially created for OpenStack and other cloud environments. It is a capability available on the FortiGate-VM even when booting within a VMware vCenter or standalone ESX environment. Config drive also allows the administrator to pass both day zero configuration scripts and FortiGate-VM licenses to the FortiGate on initial boot.

To pass a config drive to the FortiGate-VM, first you need to create a directory structure, and place the license file and configuration script file in the appropriate places. Here is the directory structure for this recipe:



For more information on the directory structure, see ESXi cloud init reference on page 20.

FortiGate-VM license file

The contents of the FGT-VM license file go into the 0000 file. Generally one would cat the license file and redirect the output into the config-drive/openstack/content/0000 file.

```
fgt-user@ubuntu:/var/tmp$
```

```
fgt-user@ubuntu:/var/tmp$ cat config-drive/openstack/content/0000
-----BEGIN FGT VM LICENSE——
#-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-#
#-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-#
#-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-#
-----END FGT VM LICENSE——
fgt-user@ubuntu:/var/tmp$
```

FortiGate configuration script

The configuration script for a FortiGate-VM uses standard FortiOS CLI syntax.

Here is a simple example below, where the hostname is Example-Day0 and port1 is configured to use DHCP to get an IP address.

```
cat config-drive/openstack/latest/user_data
#Example FGT Day0 Configuration
config system global
set hostname Example-Day0
end

config system interface
edit port1
set mode dhcp
set allowaccess https ssh ping
end
fgt-user@ubuntu:/var/tmp$
```

Creating the config drive ISO

1. Create the config-drive ISO using a utility such as xorriso. (Other utilities can be used to create ISOs such as mkisofs. Using xorriso this example refers to the config-drive directory created above with the relevant license file and configuration script. Here is an example of creating a config-drive ISO on an Ubuntu host:

   ```
   xorriso -as mkisofs -V config-2 -o Day0-CFG-Drive.iso config-drive/
   xorriso 1.3.2 : RockRidge filesystem manipulator, libburnia project.
   Drive current: -outdev 'stdio:Day0-CFG-Drive.iso'
   Media current: stdio file, overwriteable
   Media status : is blank
   Media summary: 0 sessions, 0 data blocks, 0 data, 14.3g free
   xorriso : WARNING : -volid text does not comply to ISO 9660 / ECMA 119 rules
   Added to ISO image: directory '/'='/var/tmp/config-drive'
   xorriso : UPDATE : 5 files added in 1 seconds
   xorriso : UPDATE : 5 files added in 1 seconds
   ISO image produced: 185 sectors
   Written to medium : 185 sectors at LBA 0
   Writing to 'stdio:Day0-CFG-Drive.iso' completed successfully.

   ls -l Day0-CFG-Drive.iso
   -rw-rw-r-- 1 fgt-user fgt-user 378880 Feb 15 13:32 Day0-CFG-Drive.iso
   ```

2. Place the ISO on the datastore so that it can be used with FortiGate-VMs.

3. Deploy the FortiGate-VM using an OVF template.
4. Accept the EULA, define your storage policy along with the virtual disk format, and pick the network configuration. Once you reach the end of the OVF template deployment, ensure that you deselect *Power on after deployment*. This is so we can attach our config-drive ISO as a cdrom device before initial boot.
5. Edit the VM settings.
6. Add a new device: *CD/DVD drive* and ensure that you select *Connect at power on*.
7. Attach the Day0-CFG-Drive.iso ISO that you created earlier.
8. Complete your changes, then navigate to the VM to boot it.

Results and verification

Boot the FortiGate-VM and open the console to verify that the VM is booting and utilizing the license file and day zero configuration file that was provided. Follow these verifications steps:

1. Power on the VM.
2. Go to the Console. Verify that you see the `VM license install succeeded` message and subsequent reboot.
3. Upon completion of the boot sequence, you can verify that the FortiGate-VM hostname has changed to `Example-Day0`. Also verify that the license file has been verified and the license registration status has changed to `VALID`.
4. After logging in, use the `get system status` command to verify that the license is valid.
5. Use the `get system interface physical` to verify that port1(configured in DHCP mode) has received an IP address from the DHCP server.
6. Attempt to ping fortiguard.com to confirm that the FortiGate-VM can contact Fortinet for licensing and updates.

ESXi cloud init reference

For ESX the utility xorriso is used on a Linux host to create the ISO used to boot the VM. The directory structure used to create the ISO is described below.

After the ISO is created you must upload it to your datastore of choice and attach it to the FortiGate-VM after deploying the OVF but before booting it up for the first time.

```
ls -lR config-drive/
config-drive/:
total 4
drwxrwxr-x 4 fgt-user fgt-user 4096 Feb 8 16:59 openstack

config-drive/openstack:
total 8
drwxrwxr-x 2 fgt-user fgt-user 4096 Feb 8 17:07 content
drwxrwxr-x 2 fgt-user fgt-user 4096 Feb 8 17:06 latest

config-drive/openstack/content:
total 4
-rw-rw-r-- 1 fgt-user fgt-user 287 Feb 8 17:00 0000

config-drive/openstack/latest:
```

```
total 4
-rw-r--r-- 1 fgt-user fgt-user 172 Feb 8 17:06 user_data

cat config-drive/openstack/content/0000
-----BEGIN FGT VM LICENSE——
#-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED- REDACTED-#
#-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED- REDACTED-#
#-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-#
-----END FGT VM LICENSE——

cat config-drive/openstack/latest/user_data
#Example FGT Day0 Configuration

config system global
set hostname Example-Day0
end
config system interface
edit port1
set mode dhcp
set allowaccess https ssh ping end

xorriso -as mkisofs -V config-2 -o Day0-CFG-Drive.iso config-drive/
xorriso 1.3.2 : RockRidge filesystem manipulator, libburnia project.

Drive current: -outdev 'stdio:Day0-CFG-Drive.iso' Media current: stdio file, overwriteable
Media status : is blank
Media summary: 0 sessions, 0 data blocks, 0 data, 14.3g free
xorriso : WARNING : -volid text does not comply to ISO 9660 / ECMA 119 rules Added to ISO
      image:
directory '/'='/var/tmp/config-drive'
xorriso : UPDATE : 5 files added in 1 seconds xorriso : UPDATE : 5 files added in 1 seconds
      ISO
image produced: 185 sectors
Written to medium : 185 sectors at LBA 0
Writing to 'stdio:Day0-CFG-Drive.iso' completed successfully.

ls -l Day0-CFG-Drive.iso
-rw-rw-r-- 1 fgt-user fgt-user 378880 Feb 15 13:32 Day0-CFG-Drive.iso
```

Optimizing the FortiGate-VM performance

The FortiGate-VM and VMware ESXi performance optimization techniques described in this section can improve your FortiGate-VM's performance by optimizing the hardware and the VMware ESXi host environment for FortiGate-VMs' network- and CPU-intensive performance requirements.

In addition, the port4 interface's MTU is set to be compatible with the OpenStack 10 environment, which by default, has an MTU of 1446. (In the userdata.txt file, the MTU of port4 is set to 1400.) Using the same MTU setting as the OpenStack 10 environment enables the HA heartbeat interfaces to communicate effectively over the ha-sync network.

See the following for more information on RedHat OpenStack networks and MTU values:

- MTU for VLAN networks is by default 1496 Bytes in Red Hat OpenStack Platform 10
- CHAPTER 9. CONFIGURE MTU SETTINGS

SR-IOV

FortiGate-VMs installed on VMware platforms support Single Root I/O virtualization (SR-IOV) to provide FortiGate-VMs with direct access to hardware devices. Enabling SR-IOV means that one PCIe device (CPU or network card) can function for a FortiGate-VM as multiple separate physical devices (CPUs are network devices). SR-IOV reduces latency and improves CPU efficiency by allowing network traffic to pass directly between a FortiGate-VM and a network card without passing through the VMware kernel and without using virtual switching.

FortiGate-VMs benefit from SR-IOV because SR-IOV optimizes network performance and reduces latency. FortiGate-VMs do not use VMware features that are incompatible with SR-IOV, so you can enable SR-IOV without negatively affecting your FortiGate-VM.

SR-IOV hardware compatibility

SR-IOV requires that the hardware on which your VMware host is running has BIOS, physical NIC, and network driver support for SR-IOV.

To enable SR-IOV, your VMware platform must be running on hardware that is compatible with SR-IOV and with FortiGate-VMs. FortiGate-VMs require network cards that are compatible with ixgbevf or i40evf drivers.

Installing optimal network card drivers

To support SR-IOV and other optimal performance techniques, install the most up-to-date network drivers.

You can find information about the network cards installed in your host hardware from the OpenStack Horizon client or from the OpenStack CLI.

Research the most up-to-date drivers for your hardware and install them from the Horizon client or the CLI.

Creating SR-IOV virtual interfaces

Complete the following procedure to enable SR-IOV. This procedure requires restarting the VMware host and powering down the FortiGate-VM and should only be done during a maintenance window or when the network is not very busy.

If you are using the VMware host client, do the following:

1. Go to *Manage* > *Hardware* > *PCI Devices* to view all PCI devices on the host.
2. Select the *SR-IOV capable* filter to view the PCI devices (network adapters) that are compatible with SR-IOV.
3. Select a network adapter and select *Configure SR-IOV*.
4. Enable *SR-IOV* and specify the *Number of virtual functions*.
5. Save your changes and restart the VMware host.

If you are using the vSphere web client, do the following:

1. Go to the host with the SR-IOV physical network adapter that you want to add virtual interfaces to.
2. In the *Networking* part of the *Manage* tab, select *Physical Adapters*.
3. Select the physical adapter for which to enable SR-IOV settings.
4. Enable *SR-IOV* and specify the *Number of virtual functions*.
5. Save your changes and restart the VMware host.

You can also use the `$ esxcli system module parameters set -m <driver-name> -p "max_vfs=<virtual-interfaces>"` command from the ESXi host CLI to add virtual interfaces to one or more compatible network adapters, where <driver-name> is the network adapter driver name (for example ixgbevf or i40evf) and <virtual-interfaces> is a comma-separated list of number of virtual interfaces to allow for each physical interface.

For example, if your VMware host includes three i40evf network adapters and you want to enable six virtual interfaces on each network adapter, enter `$ esxcli system module parameters set -m <i40evf> -p "max_vfs=6,6,6"`.

Assigning SR-IOV virtual interfaces to a FortiGate VM

1. Power off the FortiGate-VM and open its virtual hardware settings.
2. Create or edit a network adapter and set its type to *SR-IOV passthrough*.
3. Select the physical network adapter for which you have enabled SR-IOV.
4. (Optional) Associate the FortiGate-VM network adapter with the port group on a standard or distributed switch.
5. To guarantee that the pass-through device can access all VM memory, in the *Memory* section select *Reserve all guest memory*.
6. Save your changes and power on the FortiGate-VM.

Setting up VMware CPU affinity

Configuring CPU affinity on your FortiGate-VM further builds on the benefits of SR-IOV by enabling the FortiGate-VM to align interrupts from interfaces to specific CPUs.

By specifying a CPU affinity setting for each VM, you can restrict the assignment of VMs to a subset of the available processors in multiprocessor systems. By using this feature, you can assign each VM to processors in the specified affinity set.

Using CPU affinity, you can assign a VM to a specific processor. This assignment allows you to restrict the assignment of VMs to a specific available processor in multiprocessor systems.

For example, if you are using the vSphere web client use the following steps:

1. Power off the FortiGate-VM.
2. Edit the FortiGate-VM hardware settings and select *Virtual Hardware*.
3. Select CPU options.
4. In *Scheduling Affinity*, specify the CPUs to have affinity with the FortiGate-VM. For best results, the affinity list should include one entry for each of the FortiGate VM's virtual CPUs.
5. Save your changes.

Setting up FortiGate-VM interrupt affinity

In addition to enabling SR-IOV in the VM host, to fully take advantage of SR-IOV performance improvements, you must configure interrupt affinity for your FortiGate-VM. Interrupt affinity (also called CPU affinity) maps FortiGate-VM interrupts to the CPUs that are assigned to your FortiGate-VM. You use a CPU affinity mask to define the CPUs that the interrupts are assigned to.

A common use of this feature is to improve your FortiGate-VM's networking performance by:

- On the VM host, add multiple host CPUs to your FortiGate-VM.
- On the VM host, configure CPU affinity to specify the CPUs that the FortiGate-VM can use.
- On the VM host, configure other VM clients on the VM host to use other CPUs.
- On the FortiGate-VM, assign network interface interrupts to a CPU affinity mask that includes the CPUs that the FortiGate-VM can use.

In this way, all available CPU interrupts for the configured host CPUs are used to process traffic on your FortiGate interfaces. This configuration could lead to improve FortiGate-VM network performance because you have dedicated VM host CPU cycles to processing your FortiGate-VM's network traffic.

You can use the following CLI command to configure interrupt affinity for your FortiGate-VM:

```
config system affinity-interrupt
   edit <index>
      set interrupt <interrupt-name>
      set affinity-cpumask <cpu-affinity-mask>
   next
```

Where:

<interrupt-name> the name of the interrupt to associate with a CPU affinity mask. You can view your FortiGate-VM interrupts using the `diagnose hardware sysinfo interrupts` command. Usually you would associate all of the interrupts for a given interface with the same CPU affinity mask.

<cpu-affinity-mask> the CPU affinity mask for the CPUs that will process the associated interrupt.

For example, consider the following configuration:

- Port2 and port3 interfaces of a FortiGate-VM send and receive most of the traffic.
- On the VM host you have set up CPU affinity between your FortiGate-VM and four CPUs (CPU 0, 1 , 2, and 3)
- SR-IOV is enabled and SR-IOV interfaces use the i40evf interface driver.

The output from the `diagnose hardware sysinfo interrupts` command shows that port2 has the following transmit and receive interrupts:

```
i40evf-port2-TxRx-0
```

```
i40evf-port2-TxRx-1
i40evf-port2-TxRx-2
i40evf-port2-TxRx-3
```

The output from the `diagnose hardware sysinfo interrupts` command shows that port3 has the following transmit and receive interrupts:

```
i40evf-port3-TxRx-0
i40evf-port3-TxRx-1
i40evf-port3-TxRx-2
i40evf-port3-TxRx-3
```

Use the following command to associate the port2 and port3 interrupts with CPU 0, 1 , 2, and 3:

```
config system affinity-interrupt
   edit 1
      set interrupt "i40evf-port2-TxRx-0"
      set affinity-cpumask "0x0000000000000001"
   next
   edit 2
      set interrupt "i40evf-port2-TxRx-1"
      set affinity-cpumask "0x0000000000000002"
   next
   edit 3
      set interrupt "i40evf-port2-TxRx-2"
      set affinity-cpumask "0x0000000000000004"
   next
   edit 4
      set interrupt "i40evf-port2-TxRx-3"
      set affinity-cpumask "0x0000000000000008"
   next
   edit 1
      set interrupt "i40evf-port3-TxRx-0"
      set affinity-cpumask "0x0000000000000001"
   next
   edit 2
      set interrupt "i40evf-port3-TxRx-1"
      set affinity-cpumask "0x0000000000000002"
   next
   edit 3
      set interrupt "i40evf-port3-TxRx-2"
      set affinity-cpumask "0x0000000000000004"
   next
   edit 4
      set interrupt "i40evf-port3-TxRx-3"
      set affinity-cpumask "0x0000000000000008"
   next
end
```

Configuring FortiGate-VM affinity packet redistribution

With SR-IOV enabled on the VM host and interrupt affinity configured on your FortiGate-VM there is one additional configuration you can add that may improve performance. Most common network interface hardware has restrictions on the number of RX/TX queues that it can process. This can result in some CPUs being much busier than others and the busy CPUs may develop extensive queues.

You can get around this potential bottleneck by configuring affinity packet redistribution to allow overloaded CPUs to redistribute packets they receive to other less busy CPUs. The may result in a more even distribution of packet processing to all of the available CPUs.

You configure packet redistribution for interfaces by associating an interface with an affinity CPU mask. This configuration distributes packets set and received by that interface to the CPUs defined by the CPU affinity mask associated with the interface.

You can use the following CLI command to configure affinity packet redistribution for your FortiGate-VM:

```
config system affinity-packet-redistribution
   edit <index>
      set interface <interface-name>
      set affinity-cpumask <cpu-affinity-mask>
   next
```

Where:

<interface-name> the name of the interface to associate with a CPU affinity mast.

<cpu-affinity-mask> the CPU affinity mask for the CPUs that will process packets to and from the associated interface.

For example, you can improve the performance of the interrupt affinity example shown in the following command to allow packets sent and received by the port3 interface to be redistributed to CPUs according to the 0xE CPU affinity mask.

```
config system affinity-packet-redistribution
   edit 1
      set interface port3
      set affinity-cpumask "0xE"
   next
```

TSO and LRO

Enable TCP Segmentation Offload (TSO) and Large Receive Offload (LRO) can improve FortiGate-VM performance by reducing the CPU overhead for TCP/IP network operations.

TSO causes network cards to divide larger data chunks into TCP segments. If TSO is disabled, the CPU segmentation for TCP/IP. TSO is also sometimes called Large Segment Offload (LSO) or Large Send Offload.

LRO reassembles incoming network packets into larger buffers and transfers the resulting larger but fewer packets to the network stack of the host or virtual machine. The CPU has to process fewer packets.

Your server hardware must support TSO and LRO.

Enabling TSO

1. On the *Manage* tab, select *Advanced System Settings*.
2. For IPv4, set *Net.UseHwTSO* to 1 to enable TSO, or to 0 to disable TSO.
3. For IPv6, set *useNet.UseHwTSO6* to 1 to enable TSO, or to 0 to disable TSO.

Enabling LRO

1. On the *Manage* tab, select *Advanced System Settings*.
2. For IPv4, set *Net.Vmxnet2HwLRO* and *Net.Vmxnet3HwLRO* to 1 to enable LRO, or to 0 to disable LRO.
3. For IPv6, set *useNet.UseHwTSO6* to 1 to enable TSO, or to 0 to disable TSO.

Hyperthreading

Enabling hyperthreading for VMware allows a single processor core to function as two logical processors, often resulting in improved performance. If your VMware server hardware CPUs support hyperthreading you may be able to optimize FortiGate-VM performance by enabling hyperthreading (sometimes called logical processor) in the server's BIOS and in VMware.

1. On the *Configuration* tab, go to *Processors* > *Properties*.
2. Turn on hyperthreading.
3. Save your changes.

Multi-queue support

Multi-queue can scale network performance with the number of vCPUs. Multi-queue can also create multiple TX and RX queues. Modify the .vmx file or access *Advanced Settings* to enable multi-queue.

To enable multi-queue, open the .vmx file and add the following parameter:

```
ethernetX.pnicFeatures = "4"
```

To enable receive-side scaling (RSS), from the ESXi CLI enter:

```
$ vmkload_mod -u ixgbe
$ vmkload_mod ixgbe RSS="4,4,4,4,4,4"
```

For the best performance, you should also add CPU threads for each ethernet/vSwitch device. The amount of spare CPU resources available on the ESXi host limits this.

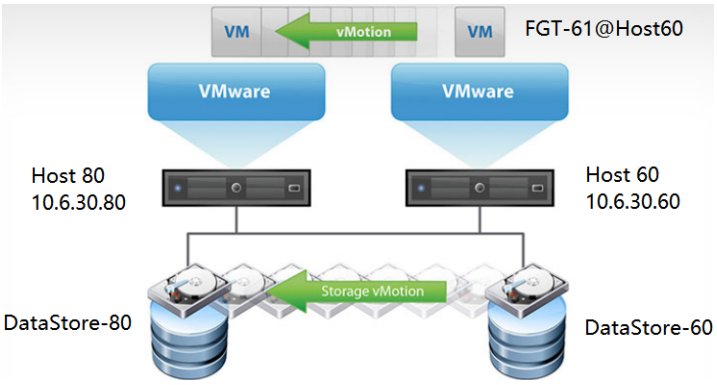
Open the .vmx file and add the following parameter:

```
ethernetX.ctxPerDev = "1"
```

vMotion in a VMware environment

This guide provides sample configuration of a vMotion FortiGate-VM in a VMware environment. VMware vMotion enables the live migration of a running FortiGate-VM from one physical server to another with zero downtime, continuous service availability, and complete transaction integrity. It also provides transparency to users.

The following depicts the network topology for this sample deployment. In this sample deployment, there are two hosts, Host 60 (10.6.30.60) and Host 80 (10.6.30.80), which are members of Cluster 1 in the DataCenter 1. DataCenter 1 is managed by the vCenter server (10.6.30.99).



The following prerequisites must be met for this configuration:

- The vCenter server has been set up and the data center and cluster have been created.
- Host 60 and Host 80 are part of the cluster.
- A Gigabit Ethernet network interface card with a VMkernel port enabled for vMotion exists on both ESXi hosts.
- A FortiGate-VM is set up and able to handle traffic.

To migrate the FortiGate-VM on the vCenter web portal:

1. Log into the vCenter web portal.
2. Verify the current location of the FortiGate-VM:
   a. Navigate to the FortiGate-VM.
   b. On the *Summary* tab, check the *Host*.In this example, the host is currently Host 60 (10.6.30.60).
   c. Go to *Storage* > *Files*. Check that the FortiGate-VM is located in the correct datastore. In this example, the datastore is currently Datastore 60, which is in Host 60.
3. Right-click the FortiGate-VM and select *Migrate*.
4. Configure the migration options:
   a. For *Select a migration type*, select *Change both compute resource and storage*. Click *NEXT*.
   b. For *Select a compute resource*, select the desired new compute resource. In this example, Host 80 (10.6.30.80) is selected. Click *NEXT*.
   c. For *Select storage*, select the storage associated with the compute resource selected in step 5. In this example, Datastore 80 (as corresponds to Host 80) is selected. Click *NEXT*.
   d. For *Select networks*, select the desired destination network at the compute resource selected in step 5. In this

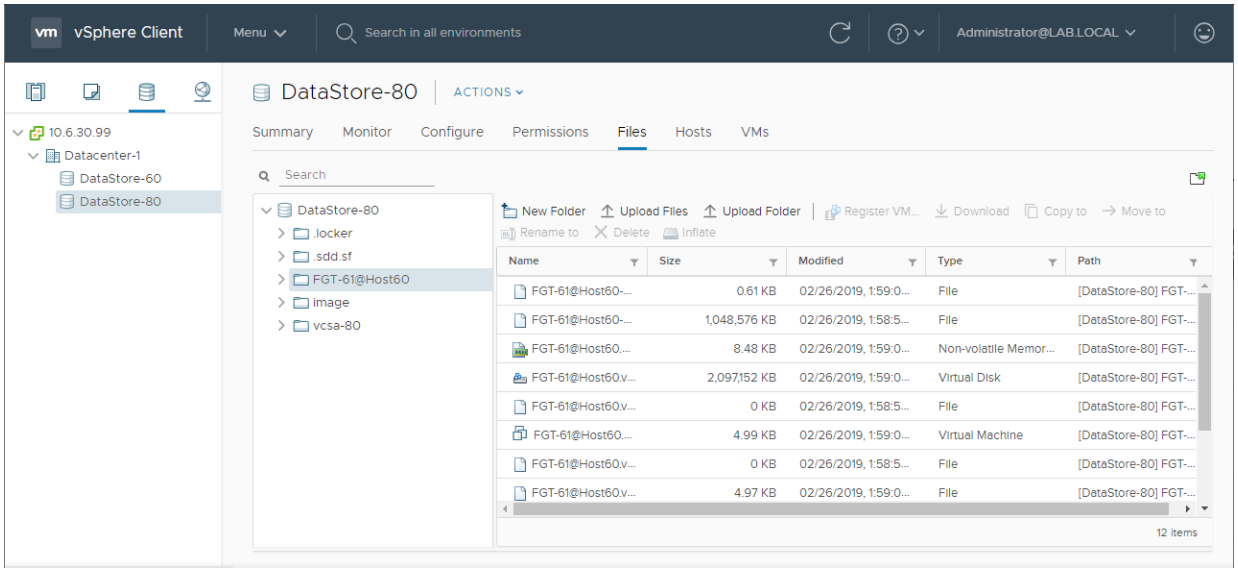
example, the source network is at Host 60, and the destination network is at Host 80. Click *NEXT*.s

e. For *Select vMotion priority*, select *Schedule vMotion with high priority (recommended)*. Click *NEXT*.

5. Before initiating the migration, open the CLI for the FortiGate-VM to check on traffic during the migration. Enter the `diag sniffer packet any 'icmp and host 8.8.8.8'` command to check if traffic is stable. If no traffic is lost during migration and the FortiGate-VM SSH session does not break, the output resembles the following:

```
FortiGate-VM64 # diag sniffer packet any 'icmp and host 8.8.8.8'
interfaces=[any]
filters=[icmp and host 8.8.8.8]
2.284655 10.1.100.22 -> 8.8.8.8: icmp: echo request
2.284704 172.16.200.61 -> 8.8.8.8: icmp: echo request
2.290014 8.8.8.8 -> 172.16.200.61: icmp: echo reply
2.290023 8.8.8.8 -> 10.1.100.22: icmp: echo reply
3.286396 10.1.100.22 -> 8.8.8.8: icmp: echo request
3.286399 172.16.200.61 -> 8.8.8.8: icmp: echo request
3.291257 8.8.8.8 -> 172.16.200.61: icmp: echo reply
3.291259 8.8.8.8 -> 10.1.100.22: icmp: echo reply
4.287616 10.1.100.22 -> 8.8.8.8: icmp: echo request
4.287620 172.16.200.61 -> 8.8.8.8: icmp: echo request
4.293134 8.8.8.8 -> 172.16.200.61: icmp: echo reply
4.293136 8.8.8.8 -> 10.1.100.22: icmp: echo reply
5.289483 10.1.100.22 -> 8.8.8.8: icmp: echo request
5.289486 172.16.200.61 -> 8.8.8.8: icmp: echo request
5.294584 8.8.8.8 -> 172.16.200.61: icmp: echo reply
5.294586 8.8.8.8 -> 10.1.100.22: icmp: echo reply
6.290972 10.1.100.22 -> 8.8.8.8: icmp: echo request
6.290976 172.16.200.61 -> 8.8.8.8: icmp: echo request
6.295467 8.8.8.8 -> 172.16.200.61: icmp: echo reply
6.295469 8.8.8.8 -> 10.1.100.22: icmp: echo reply
7.292842 10.1.100.22 -> 8.8.8.8: icmp: echo request
7.292846 172.16.200.61 -> 8.8.8.8: icmp: echo request
7.297360 8.8.8.8 -> 172.16.200.61: icmp: echo reply
7.297362 8.8.8.8 -> 10.1.100.22: icmp: echo reply
8.294735 10.1.100.22 -> 8.8.8.8: icmp: echo request
8.294742 172.16.200.61 -> 8.8.8.8: icmp: echo request
8.299282 8.8.8.8 -> 172.16.200.61: icmp: echo reply
8.299285 8.8.8.8 -> 10.1.100.22: icmp: echo reply
9.296594 10.1.100.22 -> 8.8.8.8: icmp: echo request
9.296600 172.16.200.61 -> 8.8.8.8: icmp: echo request
9.301125 8.8.8.8 -> 172.16.200.61: icmp: echo reply
9.301127 8.8.8.8 -> 10.1.100.22: icmp: echo reply
```

6. Click *FINISH*. After a few seconds, the FortiGate-VM is migrated to the new compute resources, in this case Host 80.
7. Log into the vCenter web portal. Navigate to the FortiGate-VM. On the *Summary* tab, the *Host* is now the new compute resources, in this case Host 80 (10.6.30.80).
8. Go to *Storage* > *Files*. It shows that the FortiGate-VM is now located in a new datastore, in this example Datastore 80.



To configure the FortiGate-VM using the CLI:

```
config system interface
   edit "port1"
      set vdom "root"
```

```
      set ip 10.6.30.61 255.255.255.0
      set allowaccess ping https ssh snmp http telnet
      set type physical
   next
   edit "port2"
      set vdom "root"
      set ip 10.1.100.61 255.255.255.0
      set allowaccess ping https ssh snmp http telnet
      set type physical
   next
   edit "port3"
      set vdom "root"
      set ip 172.16.200.61 255.255.255.0
      set allowaccess ping https ssh snmp http telnet
      set type physical
   next
end
config router static
   edit 1
      set gateway 172.16.200.254
      set device "port3"
   next
end
config firewall policy
   edit 1
      set srcintf "port2"
      set dstintf "port3"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set nat enable
   next
end
```

Change log

Date	Change description
2019-03-28	Initial release.